Cultures & Conflits

64 | hiver 2006
Identifier et surveiller

Bases de données personnelles et politiques de sécurité : une protection illusoire ?

Sylvia Preuss-Laussinotte

Édition électronique
URL : http://journals.openedition.org/conflits/2133
DOI : 10.4000/conflits.2133
ISSN : 1777-5345

Éditeur :
CCLS - Centre d'études sur les conflits lilberté et sécurité, L'Harmattan

Édition imprimée
Date de publication : 20 décembre 2006
Pagination : 77-95
ISBN : 978-2-296-02667-4
ISSN : 1157-996X

Référence électronique
Sylvia Preuss-Laussinotte, « Bases de données personnelles et politiques de sécurité : une protection illusoire ? », *Cultures & Conflits* [En ligne], 64 | hiver 2006, mis en ligne le 06 mars 2007, consulté le 02 mai 2019. URL : http://journals.openedition.org/conflits/2133 ; DOI : 10.4000/conflits.2133

Bases de données personnelles et politiques de sécurité : une protection illusoire ?

Sylvia Preuss-Laussinotte

1 La problématique des bases de données [1] est inséparable de l'apparition des systèmes d'identification et de surveillance de masse, qui a été parallèle à la constitution de l'Etat moderne. Les techniques de fichage ont changé au cours du temps, pour aboutir au tout informatique, dans un mouvement de « convergence » dont le langage numérique est le pivot permettant l'élaboration d'immenses bases de données personnelles. Celles-ci contiennent désormais des données biométriques (essentiellement les empreintes digitales et génétiques) et sont l'élément transversal des nouveaux systèmes d'identification, de surveillance, d'information, de communication et de protection. Publiques, privées et transnationales, elles structurent et renforcent ces systèmes. Par l'incorporation de toutes les données concernant l'identité, le corps, les relations, les mouvements, les connexions, les goûts, les préférences des individus – c'est-à-dire tout ce qui peut être considéré comme une donnée personnelle – ainsi que par leur interconnexion avec d'autres bases de données, elles sont devenues le moyen d'anticipation des comportements « à risque » et de tentative de prédiction du futur dans un monde incertain. Elles ont donc acquis un rôle central dans les politiques de sécurité.

2 En Europe, ce processus s'est accompagné d'un encadrement juridique important, dont l'efficacité reste à démontrer, la question la plus sensible étant celle de la protection effective des droits des personnes fichées. Mais la question de la sécurité technique de ces bases l'est également, bien qu'elle soit souvent passée sous silence. Ce sont ces deux aspects qui seront présentés dans cet article, dans le cadre d'une analyse juridique de l'élaboration, au niveau européen, d'une politique de sécurité fondée sur la création de bases de données personnelles.

3 Les politiques sécuritaires se matérialisent désormais par la création de bases de données internationales, européennes et nationales qui concentrent un nombre de données

gigantesques dans les domaines du contrôle des flux migratoires, de la lutte contre la criminalité et le terrorisme. La question de leur contrôle s'est posée dès l'origine : ainsi, la première grande base de données européenne, le SIS (Système d'information Schengen) [2] qui, symboliquement, mettait en place le premier fichage européen spécifique pour les étrangers [3] a fonctionné sans réel contrôle démocratique, le Comité exécutif ne tenant aucun compte des critiques qui lui ont été adressées, notamment par son Autorité de contrôle commune [4] ; ce constat reste valable aujourd'hui même si des recours internes ont ponctuellement, comme en France, permis d'obtenir quelques avancées en faveur des personnes signalées [5]. Le SIS, désormais techniquement obsolète, doit être remplacé par le SIS II, nettement plus adapté aux exigences sécuritaires actuelles puisqu'il intègre des données biométriques. Or à terme, ces bases de données intègreront prioritairement les données génétiques, si l'on se fie au traité de Prüm, signé entre sept Etats membres de l'Union européenne [6] : il est à craindre que, n'étant pas signé dans le cadre de l'Union européenne, il échappe à tout contrôle de type démocratique.

4 C'est le fichier Eurodac [7] qui va, le premier, tester l'efficacité des bases de données biométriques qui ont fonctionné à la satisfaction proclamée des institutions européennes [8]. Encouragées par ce succès, elles élaborent un nouveau fichier biométrique dans le cadre de la politique européenne de visas : le VIS [9], présenté comme prioritaire malgré quelques difficultés techniques reconnues, devrait être opérationnel bien avant le SIS II. Le choix d'intégrer aux fichiers de sécurité les données biométriques présentées comme garantes de l'authentification / identification parfaite est donc désormais acquis sans qu'aucun réel débat démocratique n'ait eu lieu.

5 Cette évolution des fichiers de sécurité vers l'intégration des données biométriques est identique en France, même si les questions techniques et budgétaires en limitent parfois la mise en place. Ainsi, la décision d'intégrer les empreintes digitales des étrangers demandant des titres de séjour prise en 1997 [10] ne s'est pas encore concrétisée dans la création d'un fichier, comme l'indique (tout en le regrettant) le rapport Mariani [11]. Du côté judiciaire et policier, l'évolution est plus ancienne, les grands fichiers de sécurité s'étant rapidement multipliés : le FPR [12], le STIC et le JUDEX [13] (qui est l'équivalent du STIC pour la gendarmerie) sont les fichiers les plus connus, centralisant des millions de noms (condamnés, suspects, victimes, témoins) ; mais de nombreux autres fichiers existent, notamment celui des renseignements généraux, de la Direction de la surveillance du territoire (DST), de la Direction générale de la sécurité extérieure (DGSE). Parallèlement, de grands fichiers biométriques ont été créés, jusqu'à présents consultés uniquement de manière complémentaire : le FAED (pour les empreintes digitales) [14] et le FNAEG (identification par empreintes génétiques) [15]. Mais, à terme, l'objectif est d'interconnecter ces fichiers, puis d'y intégrer ces données biométriques, selon la démarche européenne actuellement en cours.

6 Cette évolution est remarquable, la France étant un pays où la protection du droit à la vie privée est traditionnellement très forte. On est ainsi passé d'une longue période de réactions hostiles aux bases de données personnelles à celle de leur acceptation, puis à la certitude de leur nécessité : seules quelques résistances marginales se sont manifestées face au recours désormais systématique à la biométrie en matière de documents d'identité, et à la mise en place de traitements de ces données. La résistance au fichage s'est parfois transformée en revendication du fichage : il en a été ainsi pour le fichier d'empreintes génétiques des délinquants sexuels qui n'a fait l'objet d'aucune opposition. Le consensus a en effet été général, malgré quelques voix dissidentes rappelant que les

expérimentations effectuées sur une partie de la population se généralisent rapidement à son ensemble. Les résistances liées à l'extension considérable et parfaitement prévisible du fichage génétique sont récentes et ne sont apparues que lorsque des syndicalistes condamnés pour des actions militantes ont eu l'obligation de subir un prélèvement d'ADN et ont refusé de s'incliner, commettant ainsi le délit prévu à l'article 706-56 II du code de procédure pénale. La découverte récente de l'objectif non caché du FNAEG – le Fichage du maximum de personnes – peut surprendre par sa tardiveté [16]. Elle est caractéristique de l'acceptation actuelle du fichage au nom de la sécurité conçue de manière très large.

7 L'aspect juridique de la notion de sécurité est rarement évoqué : elle est généralement renvoyée à des analyses de type sociologique ou de philosophie politique. On ne peut pourtant pas aborder les questions posées par les fichiers de sécurité sans tenter de cerner son sens juridique.

8 Il nous semble utile en préliminaire de relever un contre-sens qui tend à se répandre, et qui figure de longue date dans les discours des hommes politiques pour justifier les mesures de restriction aux libertés au nom de la sécurité : l'existence d'un prétendu « droit à la sécurité ». On relève parfois même une confusion entre « droit à la sûreté » (article 9 de la Déclaration des droits de l'Homme de 1789 [17]) et un prétendu « droit à la sécurité », alors que ces deux notions sont antinomiques. En effet, dans une interprétation stricte, le droit à la sûreté renvoie à l'Habeas corpus anglais, si malmené au Royaume-Uni depuis les attaques terroristes et la nouvelle politique sécuritaire anglaise ; il interdit toute arrestation, toute détention arbitraire et se concrétise par l'obligation de présenter la personne arrêtée dans les plus brefs délais devant un juge qui statuera sur une éventuelle détention. Jean Rivero en donne une définition plus générale, qui la situe clairement dans la confrontation de l'individu au pouvoir :

> « La sûreté est beaucoup plus qu'une liberté particulière ayant un objet déterminé [...] elle est, plus largement, la garantie de la sécurité juridique de l'individu face au pouvoir. [...] La sûreté constitue donc la protection avancée de toutes les libertés : c'est elle qui permet leur exercice paisible [18] ».

9 Thomas Hobbes [19], qui a théorisé de la manière la plus radicale l'importance de la sécurité dans le contrat social, l'a clairement décrite comme un attribut de l'Etat. C'est en échange de l'abandon par les hommes de toutes les libertés qu'ils possédaient dans l'état de nature – l'absence de limite à ces libertés entraînant une insécurité permanente – que le Leviathan va assurer leur sécurité, qui est au fondement même du contrat social. Hobbes ne reconnaît qu'une seule réserve à cet abandon général des libertés au Prince : le droit à la sûreté, autrement dit l'interdiction des arrestations et détentions arbitraires, seul droit que les hommes conservent.

10 Il ne s'agit pas ici d'un débat sur les notions générales de sûreté et de sécurité, bien difficile, mais sur la notion juridique de « droit à la sûreté », qui est très claire, et d'un prétendu « droit à la sécurité » extrêmement dangereux par le risque de confusion qu'il entraîne entre les domaines de la protection des droits et celui de la sécurité. Il est donc inquiétant de voir réapparaître aujourd'hui ce prétendu « droit à la sécurité » [20], pourtant conceptuellement opposé aux droits fondamentaux. Est-il besoin de rappeler que dans tous les textes internationaux de protection des droits, la sécurité est toujours entendue comme autorisant l'Etat à restreindre les droits et libertés ? Ainsi, la sécurité est citée dans la Cour européenne des droits de l'Homme comme autorisant des restrictions par l'Etat à un ensemble de libertés et permettant même dans des cas extrêmes (état d'urgence, conflits, etc.) d'y déroger, sauf quatre hypothèses prévues à l'article 15 : droit à

la vie (article 2), interdiction des tortures et peines ou traitements inhumains ou dégradants (articles 3), interdiction de l'esclavage et de la servitude (article 4), non rétroactivité de la loi pénale (article 7). C'est d'ailleurs ce dilemme qui est au cœur des débats actuels : jusqu'où la sécurité autorise-t-elle des atteintes aux droits fondamentaux sans atteindre, voire détruire, l'essence même de l'Etat démocratique [21] ? Les expériences totalitaires qui se sont toutes fondées sur le droit pour accompagner leurs dérives en arguant de la sécurité doivent faire réfléchir.

11 L'un des acquis les plus importants de l'Etat de droit est précisément la relation équilibrée construite entre la sécurité et la démocratie, entre sécurité et droits fondamentaux. Et c'est bien à partir de cette relation que l'on doit aborder la question de l'encadrement juridique des technologies et fichiers de sécurité. La Cour européenne des droits de l'Homme, qui élabore de véritables normes destinées à définir ce qu'est la démocratie au sens européen, tente de répondre à cette question fondamentale. Si elle reconnaît que dans une société démocratique, « les intérêts de la sécurité nationale prévalent [...] sur les intérêts individuels [22] », elle est particulièrement attentive à définir les limites qui ne doivent pas être franchies au nom de la sécurité, notamment en matière de fichage. Ainsi, « le pouvoir de surveiller en secret les citoyens n'est tolérable [...] que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques [23] ». Il s'agit là du « degré minimal de protection voulu par la prééminence du droit dans une société démocratique ». Et la Cour a toujours réaffirmé cette position, notamment dans un arrêt récent à propos de données personnelles liées aux opinions politiques contenues dans un fichier de sécurité [24].

12 Le Conseil constitutionnel français n'a par contre jamais recours au concept de sécurité lorsqu'il est saisi de lois qui, pourtant, comportent ce terme dans leur intitulé [25]. Il utilise classiquement l'expression d'« ordre public », notion aussi floue qu'extensive, dont il a fait un objectif de valeur constitutionnelle destiné à justifier les restrictions aux libertés, notamment au respect de la vie privée en matière de fichiers de sécurité [26]. Il est particulièrement intéressant de noter cette présentation de la notion d'ordre public dans le cadre d'un des séminaires des Cours constitutionnelles :

> « Le Conseil constitutionnel n'a jamais défini ce qu'il entendait par ordre public... Mais, à la lecture de ses décisions, il est facile de comprendre ce à quoi il fait référence. Il s'agit en fait d'une notion que tout le monde comprend sans qu'il soit besoin de lui donner une définition précise ! [27] »

13 On peut en conclure que le Conseil n'innove pas et se réfère à la notion française classique d'ordre public liée au pouvoir de police générale, dont la sécurité fait partie puisqu'il comprend « le bon ordre, la sécurité, la salubrité et la tranquillité publique ».

14 On notera enfin que, malgré ce flou conceptuel, et si l'on veut tenter d'appréhender juridiquement une certaine vision actuelle de la sécurité, il peut être utile de se référer à un principe juridique apparu récemment, d'abord au niveau européen, puis repris par le juge français et désormais constitutionnalisé [28] : le principe de précaution, que l'on a essentiellement développé en matière d'environnement et qui justifie progressivement la mise en place d'un véritable encadrement juridique. C'est bien au nom d'un véritable principe de précaution que l'on a en effet introduit un ensemble de technologies de sécurité et que l'on recourt de manière exponentielle aux bases de données, devenues le moyen d'anticipation des comportements « à risque ». On a ainsi basculé dans un univers de « précaution » omniprésente.

15 La relation entre sécurité et démocratie étant centrale, l'Europe a fait le choix d'aborder la question des fichiers de sécurité sous l'angle du respect des personnes au regard des atteintes possibles à leurs droits. Mais si les textes de protection sont nombreux, ils sont souvent peu lisibles, d'autant que les organismes français et européens chargés du contrôle de leur application produisent une multitude d'avis, analyses, commentaires qui n'ajoutent pas à la clarté, et dont l'efficacité peut laisser dubitatif.

16 La contrepartie au fichage des personnes dans les traitements de sécurité a toujours été posée en termes de protection de la vie privée, abordée plus ou moins rigoureusement selon les Etats. Les pays d'Europe continentale comme l'Allemagne et la France en ont une vision très forte, alors que les pays de tradition anglo-saxonne, comme l'Angleterre et les Etats-Unis, l'abordent avec beaucoup plus de souplesse. C'est en France que cette protection est la plus forte : construite progressivement à partir du xixe siècle par les juges civils sur la base de la responsabilité délictuelle (article 1382 du code civil), elle a été introduite en 1970 par la loi tant sur le plan civil (article 9 du code civil) que pénal (article 226 et suivants du code pénal). Le Conseil constitutionnel en a fait un droit autonome, rattaché aux articles 2 et 4 de la Déclaration des droits de l'Homme de 1789, et l'a essentiellement utilisé dans le cadre de son contrôle en matière de fichiers de sécurité (voir note 11).

17 Cette conception forte du droit à la vie privée se rapproche de la position développée par la Cour européenne des droits de l'Homme à partir de l'article 8 de la CEDH [29]. Considéré comme un droit-carrefour, l'article 8 a permis à la Cour européenne de développer une jurisprudence particulièrement diversifiée de la protection de la vie privée, en l'étendant à certaines technologies de sécurité. Ainsi, la France a été condamnée deux fois, à quinze ans d'intervalle, pour sa législation insuffisamment précise en matière d'interception de communications [30]. Le Royaume-Uni l'a été pour les excès de son système de vidéosurveillance, permettant d'utiliser les images qui en sont issues sans considération véritable de la protection de la vie privée des personnes filmées [31].

18 Cela dit, la définition exacte de ce qu'est la vie privée n'est pas uniforme. Selon un rapport de l'OCDE sur les technologies fondées sur la biométrie [32], fortement inspiré par la conception américaine dominante en matière de technologies de sécurité, « la protection de la vie privée va du simple droit de s'isoler [« right to be left alone »] au droit qu'ont les personnes de créer et de maintenir un "espace privé" autour d'elles, tant physique que numérique, protégé des interférences des autres » (Warren and Brandeis, 1890). Cette référence aux Etats-Unis dans un texte de portée internationale n'est pas neutre : si les USA protègent la liberté d'expression de manière presque absolue, ils sont par contre nettement moins attentifs à la protection de la vie privée, notamment en matière de données personnelles destinées aux fichiers de sécurité. Non prévu par la Constitution américaine, le droit à la vie privée a été rattaché par la Cour suprême au quatrième amendement. Mais il est exclu que le gouvernement fédéral intervienne dans le secteur privé pour lui imposer une réglementation – notamment en matière de données personnelles –, ce qui signe une opposition claire avec la conception européenne. Une seule loi fédérale existe, applicable au secteur public : la Loi sur la vie privée de 1974 (Privacy Act of 1974) qui protège les données détenues dans les fichiers des agences gouvernementales américaines, notamment de sécurité, et impose à ces agences le respect de certaines pratiques. Mais l'efficacité de cette loi est considérablement réduite par l'absence d'une agence de surveillance et par l'interprétation administrative du texte qui permet la divulgation d'informations personnelles.

19 Cette approche explique que l'on puisse trouver sur Internet à peu près n'importe quelle information sur l'ensemble des personnes vivant aux Etats-Unis, y compris leurs condamnations pénales, mais aussi la facilité avec laquelle les agences de sécurité américaines accèdent aux données personnelles et les traitent au nom de la lutte contre le terrorisme. Malgré la connaissance de l'inexistence d'une protection américaine en matière de données personnelles la Commission européenne a publié une décision d'adéquation en se fondant sur l'existence d'un tel prétendu système aux Etats-Unis [33].

20 Le constat est simple : c'est en se fondant sur la protection des personnes que l'on justifie l'extension considérable des bases de données personnelles, y compris au niveau mondial. Or, force est de constater que cette protection, même quand elle est prévue de manière spécifique comme en Europe, est de plus en plus formelle.

21 En Europe, position difficilement compréhensible pour les Américains (pour qui ce sont les Etats qui sont les plus susceptibles de surveiller et porter atteinte à la vie privée – ce qu'ils prouvent en effet aujourd'hui), des lois portant spécifiquement sur la protection des données personnelles ont émergé depuis les années 1970. On a ainsi assisté à leur autonomie progressive par rapport à la généralité du concept de droit à la vie privée. La protection des données personnelles représente désormais un domaine indépendant, aujourd'hui très construit juridiquement dans le cadre de l'Union européenne et de ses Etats membres, et très présent, formellement du moins, dans le cadre des fichiers de sécurité.

22 Le concept de données personnelles a pris de l'ampleur, les textes en donnant des définitions très larges [34]. Ainsi actuellement, un consensus existe sur le fait d'assimiler une donnée biométrique à une donnée personnelle. Par contre, les données personnelles issues de la vidéosurveillance en sont expressément écartées par le considérant 16 de la directive du 24 octobre 1995 [35] ; de même, l'article 10-I de la loi du 21 janvier 1995 modifiée sur la vidéosurveillance a prévu que seuls les enregistrements conservés au-delà d'un mois doivent faire l'objet d'une déclaration à la CNIL – autrement dit, la plupart des enregistrements échappent à son contrôle. Il serait pourtant plus cohérent de leur appliquer les textes de protection sur les données personnelles, afin d'unifier le régime juridique de l'ensemble des technologies de sécurité : le recours à la vidéosurveillance utilisant le protocole IP, qui donne accès aux caméras ou au système de stockage des données à partir de simples ordinateurs connectés à Internet depuis n'importe quel pays du monde, est désormais systématique dans le domaine privé et s'étend au domaine public. On parvient sans difficulté à créer d'immenses bases de données personnelles à partir des images. La CNIL souhaitait l'unification du régime de la vidéosurveillance sous l'empire de la loi du 6 janvier 1978, mais le législateur n'a pas suivi son avis [36].

23 Il est vrai qu'en France, on est passé d'un système concentré presque exclusivement sur le contrôle des fichiers publics à une logique de surveillance publique nettement moins contrôlée. La loi du 9 juillet 2004 modifiant la loi française du 6 janvier 1978 a institué une distinction entre les bases de données personnelles publiques ou privées : les fichiers publics de sécurité ne dépendent globalement plus de l'autorisation de la CNIL, notamment ceux qui contiennent des données biométriques, alors que de telles données dans un fichier privé doivent toujours obtenir son autorisation. La CNIL doit certes être saisie et son avis doit être publié, mais c'est un décret en Conseil d'Etat qui accordera l'autorisation, qui peut être prise contre cet avis, ce qui a été le cas pour de nombreux fichiers récents [37]. On notera que la CNIL a développé une position très ferme sur la constitution de bases de données biométriques : les caractéristiques biométriques ne

doivent être conservées que sur un support individuel, en aucun cas dans une base de données regroupant les caractéristiques d'autres personnes. La CNIL ne déroge à cette position que pour de sérieux motifs de sécurité : elle n'a pourtant pas accepté que le recours aux empreintes digitales pour les aéroports de Paris soit relié à une base de données. En conséquence, ADP [38] a accepté que le gabarit de l'empreinte digitale ne soit stocké que sur une carte individuelle (badge) détenue par l'employé concerné (délibération 04-017 du 08 avril 2004).

24 Cette évolution française souligne que si la protection des données personnelles semble extrêmement précise dans les textes, dans les faits, elle apparaît comme étant très formelle et peu efficace, surtout dans le cadre des fichiers de sécurité. Ce constat peut être appliqué à l'Europe.

25 L'article 25 de la directive du 24 octobre 1995 exige que tout transfert de données personnelles vers des Etats tiers à l'Union européenne ne peut s'effectuer que si ceux-ci possèdent une protection « adéquate » en matière de données personnelles, alors que les Etats de l'UE doivent disposer d'une protection « équivalente » beaucoup plus exigeante, respectant la directive de 1995 ; l'appréciation de cette condition d'adéquation est confiée à la Commission européenne. Les prévisions pessimistes sur la portée de cette évaluation se sont vérifiées, lorsque la Commission l'a retenue en faveur des Etats-Unis, malgré les résistances sévères du Parlement européen et des autorités de protection [39].

26 Cette exigence de protection adéquate, apparaît de plus très aléatoire depuis l'arrêt « Bodil Lindqvist » de la Cour de justice des Communautés du 6 novembre 2003 (C 101/01), qui semble vider l'article 25 de son sens, puisque la Cour a précisé que l'exigence de « protection adéquate » ne s'applique pas aux données personnelles circulant sur le réseau internet à destination ou en provenance de pays tiers à l'Union européenne. Il y a là un argument de bon sens : une telle exigence bloquerait la circulation transfrontière des données sur Internet, le réseau étant mondial, puisqu'il faudrait exiger de tous les pays du monde la preuve qu'ils possèdent une protection adéquate en matière de données personnelles, ce qui est irréalisable. Cette jurisprudence laisse donc le champ libre aux transferts de données sans contrôle – qu'elles soient destinées à des instances de sécurité étatiques, et/ou au commerce de fichiers de clientèle.

27 En outre, la directive du 24 octobre 1995 prévoit explicitement la possibilité pour les Etats de déroger à ses dispositions, soit parce qu'étant dans le champ communautaire, ils renvoient à la sécurité [40] – ce qui est le cas... des fichiers de sécurité –, soit parce que les bases de données dépendent du troisième pilier « coopération policière et judiciaire pénale [41] ». Lorsque le fichier dépend du premier pilier communautaire – comme Eurodac et bientôt le VIS – c'est donc la directive de 1995 qui s'applique, alors que les grands fichiers de police tels que le SIS ou Europol ne dépendent pas de cette directive. Cette distinction entre la protection des données selon le pilier dont dépend le fichier est source d'une grande complexité, accentuée par le morcellement des protections existant actuellement dans le cadre des bases de données dépendant du troisième pilier. Chaque convention créant une base de données met en place une protection qui lui est propre, certes en référence commune à la Convention STE 108 du Conseil de l'Europe [42], mais en créant des systèmes de protection internes globalement contestables et contestés, y compris par les autorités de contrôle communes (ACC) qui devraient en être les garantes, et dont le rôle est inexistant et contourné. Les rapports ou simples prises de position de ces autorités de protection, comme celles d'Alex Türk, ancien président de l'ACC Schengen (voir note 2), puis de l'ACC Europol [43] sont de manière générale très négatives

sur l'effectivité de la protection des droits dans ce cadre. Malgré le souhait de la Commission et du Parlement européen d'étendre la protection de la directive de 1995 au troisième pilier, c'est la solution d'un texte de protection spécifique sous forme de décision-cadre qui a été retenue, ce qui ne simplifiera pas la situation actuelle [44].

28 On peut donc constater que globalement, la protection des données personnelles est décevante malgré – ou à cause ? – de la profusion des textes. Aucun d'eux ne protège sérieusement les bases de données des extensions sécuritaires qui se développent extrêmement rapidement : que sont des contrôles ponctuels face à des millions, voire des milliards, de données personnelles, qui s'échangent et peuvent être modifiées à tout instant ?

29 La sécurité technique des bases de données personnelles de manière générale, et plus particulièrement dans le cadre des fichiers de sécurité « sensibles » renfermant des données biométriques, est une préoccupation majeure aujourd'hui au niveau européen comme national. Leur fragilité est en effet indéniable, quoiqu'en disent les déclarations publiques.

30 Une des questions essentielles est celle de l'authentification des personnes habilitées à accéder aux données, ainsi que les moyens de lutter contre les accès illégaux. Elle renvoie à la sécurisation des systèmes et à l'identification efficace des habilitations. Il est devenu évident que l'identification par un simple mot de passe est devenue insuffisante et justifie le choix du recours à la biométrie. Philippe Wolf [45], s'étonnant de la fascination pour les techniques biométriques au détriment de la cryptographie [46], s'étonne également du peu d'études de faisabilité dans le domaine. Or, celles qui ont été effectuées démontrent déjà que de nombreuses techniques permettent de passer outre les mécanismes de sécurité reposant en tout ou partie sur la biométrie. Pour Wolf,

31 « la publication sur Internet ou dans des cercles plus restreints d'une photographie du ou des doigts d'une personne, ou pire encore d'un fichier normalisé des points caractéristiques de cette empreinte biométrique, permet d'usurper, à peu de frais, l'identité de cette personne ».

32 Il est également possible d'usurper les mécanismes reposant, par exemple, sur la forme de la main, celle du visage, et même l'ADN d'une personne. Sans même s'attaquer au processus de la reconnaissance biométrique, il suffit pour cela de le désactiver par une attaque désignée par les agences de sécurité sous l'expression « déni de service » (le recours à la violence physique de base), ou encore en piratant le compte d'une personne qui s'est authentifiée de manière tout à fait licite.

33 Cette question rejoint une observation : un ensemble d'entreprises privées ont d'ores et déjà traité des milliards d'empreintes digitales, transcrites dans de gigantesques bases de données. De plus, la plupart des pays se sont dotés de systèmes d'identification par empreintes digitales (ou sont en passe de l'être), et de documents d'identité biométriques reliés à des bases de données, notamment du fait des exigences dans le domaine de l'aviation civile : les normes appliquées aux documents de voyage sont celles de l'OACI [47] à l'origine de la décision, prise au niveau mondial, de recourir à la biométrie (image faciale et empreintes digitales [48]) Cette décision s'applique aux cent quatre-vingt neuf Etats membres, dont un ensemble d'Etats pourtant désignés comme étant à risque en matière de terrorisme (Afghanistan, Iran, Pakistan, etc.). Or, ces éléments biométriques sont intégrés dans des bases de données nationales interconnectées mondialement.

34 Les empreintes digitales (et bientôt les empreintes génétiques [49]) sont donc devenues de véritables données publiques, stockées dans un nombre considérable de systèmes informatiques, qu'ils soient d'ailleurs publics ou privés. Or, selon Philippe Wolf [50], la fraude la plus difficile à contrôler serait le détournement de ces bases de données personnelles stockant les identifiants biométriques. La multiplication de fichiers biométriques irait donc à l'encontre de la sécurité des systèmes. Pourtant, compte tenu des choix étatiques et mondiaux en faveur de la biométrie et de l'intérêt des entreprises dans le domaine [51], on peut avancer l'hypothèse plausible d'un choix délibéré des Etats de ne pas effectuer de véritables études sur la faillibilité de ces systèmes, tout en préconisant un renforcement de leur sécurité. Cette analyse est rejointe par celle du groupe FIDIS (Future of Identity in the Information Society) qui a élaboré une Déclaration de Budapest [52], où le groupe met solennellement en garde les responsables de l'UE sur la décision de recourir aux documents de voyage biométriques compte tenu des menaces pour la sécurité des personnes, de leur vie privée et du vol d'identité.

35 La sécurité de l'information devient ainsi une préoccupation prioritaire de l'UE, notamment dans le domaine des systèmes d'information se rapportant aux grandes missions de sécurité (contrôle des frontières, gestion des flux migratoires, lutte contre le terrorisme et grande criminalité avec Europol). La gestion des risques pose des questions techniques et juridiques dont l'importance est telle que l'UE a créé une Agence européenne chargée de la sécurité des réseaux et de l'information s'adressant de manière très symptomatique aux Etats comme aux entreprises [53]. Dans chaque fichier de sécurité, l'Union européenne met à la charge des Etats un ensemble d'obligations juridiques liées à la sécurité des systèmes et des échanges. En France, le gouvernement a édité un « plan de renforcement de la sécurité des systèmes d'information de l'Etat » le 10 mars 2004, qui indique quelles mesures doivent être prises – ce qui constitue une première démarche allant dans le sens de l'unification réclamée par l'UE. Mais la question de la sécurité des systèmes est réglée par le recours à des sous-traitants par le biais de marchés publics, avec cahiers des charges très précis, et contrôle interne suivi : on retrouve toutefois ici la question centrale de la place et du contrôle des entreprises privées chargées de véritables missions de puissance publique.

36 Cette volonté de sécurisation pose aussi la question de l'interopérabilité des systèmes et donc des normes applicables, qui ne sont pas toujours les mêmes selon les Etats. Pour la sécurité des systèmes d'information, la norme de référence ISO devrait être la norme 17799 (Code of Practice for Information Security Management), ex-norme anglaise BS 7799 qui a été adoptée internationalement. Mais il est clair que l'unification n'est pas effective : au cœur même des agences publiques de sécurité françaises, les normes utilisées sont souvent différentes. Ainsi en France, la gendarmerie et la police n'utilisent pas forcément les mêmes normes, ce qui est source de difficultés. Or, les textes européens permettent d'engager la responsabilité de l'Etat qui n'aurait pas rempli ses obligations dans ce domaine.

37 Mais on retrouve ici le paradoxe déjà dénoncé : pour fonctionner efficacement, les bases de données doivent être interopérables, ce qui renforce leur fragilité, par le recours aux mêmes normes de sécurité.

38 Une des questions importantes posées par les bases de données est liée à l'utilisation qui sera faite des données personnelles qui s'y trouvent. Pour la CNIL, la finalité des bases de données doit être clairement définie et respectée. Cependant, on remarque que, dans la pratique, soit par leur interconnexion, soit par des accès des services plus larges et non

autorisés officiellement, les données peuvent être utilisées pour d'autres objectifs. C'est ce qu'un rapport de la Commission européenne sur la biométrie désigne comme étant un « détournement d'usage » (fonction creep) en le signalant comme l'un des dangers des nouveaux systèmes d'identification et de surveillance reposant sur des bases de données [54].

39 Il s'agit donc de dérives qui n'ont rien d'exceptionnel. Face à l'évolution extrêmement rapide des technologies de sécurité, dans le contexte sécuritaire actuel et au regard des exigences liées à la coopération policière et judiciaire pénale européenne, les systèmes de protection mis en place peuvent aboutir à leur contournement par une série de pratiques : création de systèmes / fichiers de données personnelles non déclarés, qui paraissent d'autant plus dangereux pour les libertés qu'ils sont clandestins, pratiques non autorisées d'accès aux bases de données, etc. Ce type de contournement a déjà été dénoncé, par exemple dans le cas d'Europol :

> « Il arrive également que, sous couvert de soutien technique, l'Office et les Etats membres mettent en place des fichiers préfigurant de possibles fichiers d'analyse sans recourir à la procédure prévue par la Convention pour la création de tels fichiers. Cette pratique est désignée dans le jargon européen par le terme de "MSOPES" ("Member State Operationnal Projects With Europol Support" que l'on pourrait traduire par "organisation mutuelle de fichiers d'analyse entre le système central d'Europol et les autorités nationales"). L'Autorité de Contrôle Commune est ainsi contournée et mise devant le fait accompli. Il lui est plus difficile de contrôler ces échanges de données. Ses observations éventuelles ont également moins de chance d'être prises en considération [55] ».

40 En France, ces détournements / contournements potentiels, qui ont déjà existé notamment avec la création du STIC et de JUDEX en dehors de tout contrôle, posent la question des extrêmes difficultés de contrôle de la CNIL, qu'elle dénonce elle-même (manque de moyens, manque de personnel, notamment de techniciens) ce qui limite ses possibilités de sanctionner ces dérives potentielles.

41 La question des erreurs contenues dans les données est également centrale, les risques de saisie incorrecte, d'homonymie ou d'erreur n'étant pas négligeables. La CNIL a clairement exprimé sa position très réservée vis-à-vis du recours aux bases de données dans le domaine de la sécurité, arguant ne pas avoir les moyens d'assurer un contrôle efficace des fichiers qui se multiplient. Elle a donné pour exemple la question soulevée par l'utilisation et la mise à jour du fichier STIC lequel, lors d'un audit en 2004, contenait 26 % d'erreurs (des milliers de personnes étaient inscrites par erreur dans le fichier) [56]. Or la loi sur la sécurité intérieure de 2003 a autorisé les consultations administratives de ces fichiers. Il s'agit là d'un des exemples de dérive des consultations de fichiers qui peut aboutir à de graves atteintes à la présomption d'innocence. Ces erreurs, homonymies, etc. sont également nombreuses dans les grands fichiers européens de sécurité, notamment le SIS qui fonctionne déjà depuis plusieurs années.

42 En France, il est toujours d'actualité de dénoncer l'interconnexion des fichiers. De fait, ces interconnexions si délicates au regard de leurs effets pour les personnes fichées sont déjà en place dans de nombreux pays européens – le Royaume-Uni en tête – alors qu'elles ne sont globalement pas autorisées en France, bien que cette interdiction soit contournée à l'aide des procédures d'accès simultané à plusieurs bases de données. Or l'Union européenne vise clairement à mettre en place une interconnexion générale tant entre les bases de données des Etats membres qu'entre les bases de données européennes dans le domaine général de la sécurité.

43 Une communication de la Commission européenne du 24 novembre 2005 relative à l'interopérabilité des bases de données européennes indique qu'elle

> « vise à montrer de quelle manière ces systèmes, en plus de leurs finalités actuelles, pourraient appuyer plus efficacement les politiques liées à la libre circulation des personnes et concourir à la réalisation de l'objectif de lutte contre le terrorisme et contre les formes graves de la criminalité ».

44 Elle est axée sur les systèmes sur lesquels le Conseil européen et le Conseil de l'Union européenne ont mis tout particulièrement l'accent dans le cadre de leur mandat, à savoir les systèmes SIS II, VIS et EURODAC qui concernent les étrangers. La Commission part du constat d'une « sous-exploitation » des possibilités offertes par ces systèmes et d'un ensemble de lacunes dont la liste est parlante : difficulté d'identification des personnes en séjour irrégulier, impossibilité d'utiliser les données relatives à l'asile, à l'immigration et aux visas à des fins de sécurité intérieure, contrôle non étendu à toutes les catégories de ressortissants des pays tiers, surveillance incomplète de l'entrée et de la sortie des ressortissants de pays tiers, absence d'outils d'identification biométrique, absence d'enregistrement des citoyens de l'Union au niveau européen, aucune base de données permettant l'identification des victimes de catastrophes et des corps non identifiés. Partant de ces constats, la Commission a proposé une série de solutions, essentiellement « le regroupement des activités de gestion quotidienne de ces systèmes au sein d'une seule et même organisation [57] ».

45 Mais ce rêve européen rencontre des difficultés. On en donnera pour illustration la mise en place d'un casier judiciaire européen – qui ne peut se construire qu'avec l'interconnexion des casiers judiciaires nationaux. Devant les obstacles, le Conseil de l'Union européenne a proposé la création d'un nouveau concept, extrêmement complexe, destiné à contourner les réticences nationales à ce type d'interconnexion : le « principe de disponibilité ». Il est présenté comme étant un nouveau principe juridique important introduit dans le programme de La Haye. Selon le CEPD, il s'agirait d'un principe simple :

> « les informations accessibles à certaines autorités dans un Etat membre doivent également être communiquées aux services équivalents des autres Etats membres. Ces informations doivent être échangées aussi rapidement et aussi facilement que possible entre les services des Etats membres et de préférence dans le cadre d'un accès en ligne [58] ».

46 Sont ainsi prévus les communications/échanges sur les profils ADN, « c'est-à-dire les codes alphanumériques composés à partir des sept marqueurs d'ADN de l'ensemble européen de référence (European Standard Set) définis dans la résolution du Conseil 2001/C 187/01 du 25 juin 2001 relative à l'échange des résultats des analyses d'ADN ». Ces marqueurs ne peuvent contenir « aucune information sur des caractéristiques héréditaires spécifiques » (selon le souhait du CEPD, celle des empreintes digitales, des numéros de téléphone et autres données relatives aux communications, à l'exclusion de données sur le contenu des communications et de données relatives au trafic, à moins que ces dernières ne soient contrôlées par une autorité désignée ; données minimums en vue de l'identification des personnes figurant dans les registres de l'état civil, etc.

47 Les questions liées aux bases de données personnelles en matière de sécurité sont immenses. Un rapport rédigé en 2003 pour la Commission européenne s'inquiète d'ailleurs des difficultés liées au recours massif à des technologies de sécurité et propose la création d'un « Observatoire européen des technologies liées à l'identité » comme solution appropriée aux risques de plus en plus évidents de dérives multiples des bases de données personnelles [59]. Mais si cette solution – relative, un observatoire n'est doté

d'aucun pouvoir – peut être intéressante, il reste qu'une question juridique n'est pas résolue : qu'est-ce que l'identité au regard du droit ? Les fichiers de sécurité, où l'on est préoccupé de manière prioritaire par l'identification, entretiennent une confusion entre celle-ci et l'identité de la personne. En France, cette question n'est pas posée – la jurisprudence du Conseil constitutionnel n'envisage l'identité que sous l'angle de la vie privée, sans que le contenu de celle-ci soit clairement défini, l'identité semblant là aussi n'être appréhendée que sous l'aspect « identification », qui fige l'identité d'une personne à un moment immobile, sans prendre en compte ses évolutions [60].

48 La grande question qui reste posée est néanmoins celle-ci : pourquoi, connaissant pertinemment les fragilités des bases de données personnelles, les risques connus d'erreurs, de détournement, les Etats ou les organisations comme l'Europe pratiquent-ils cette surenchère en matière de fichiers de sécurité, dont le coût est considérable, surtout depuis l'intégration des éléments biométriques, et qui nécessitent des procédures de maintien permanentes, confiées à des entreprises privées, augmentant d'autant les risques ? On retrouve bien évidemment l'ancienne obsession du contrôle des populations, désormais affiné au point de penser parvenir à un contrôle minutieux et personnalisé de chaque individu ; mais la justification de cette fuite en avant dans des systèmes très coûteux est avant tout fondée sur la croyance en un résultat : celle de la prévision fiable, et donc la prévention possible, des risques sécuritaires de quelque horizon qu'ils viennent. Cette position renvoie à une question non résolue : même à un haut niveau étatique ou international, une croyance peut-elle être rationnelle ?

NOTES

1.. Dans le cadre de l'article 2 de la Directive 96/9/CE du 11 mars 1996 concernant la protection juridique des bases de données : « on entend par "base de données" : un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou d'une autre manière ». La directive du 24 octobre 1995 sur la protection des données personnelles utilise l'expression plus ancienne de « fichier de données personnelles » : « tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ».

2.. Créé par la Convention d'application de l'accord de Schengen du 15 juin 1990

3.. Article 96 portant sur les « données relatives aux étrangers qui sont signalés aux fins de non admission ».

4.. « En dépit de toutes les initiatives prises et de toutes les propositions formulées par l'ACC, le Comité exécutif n'a pas adopté les mesures nécessaires afin de renforcer ses effectifs et ses moyens techniques et budgétaires, comme il s'y était engagé. Pour garantir un contrôle démocratique, la seule existence formelle d'une autorité indépendante ne suffit pas ; il est indispensable que cette autorité dispose des moyens et des outils

nécessaires pour fonctionner » (3e Rapport d'activité, Autorité de contrôle commune Schengen, Bruxelles, le 26 mars 1999 SCH/Aut-cont (99) 8, 2e rév.).

5.. Par exemple, arrêts du Conseil d'Etat : CE, 9 juin 1999, n°190384, époux Forabosco, et récemment CE, 7 avril 2006, n°275216, Skandrani.

6.. Traité entre le royaume de Belgique, la République fédérale d'Allemagne, le royaume d'Espagne, la République française, le Grand-Duché de Luxembourg, le royaume des Pays-Bas et la République d'Autriche relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale, signé à Prüm le 27 mai 2005, désigné comme étant un « Schengen III ». Pour des précisions, voir dans ce numéro, notre article « L'Union européenne et les technologies de sécurité ».

7.. Règl. CE n°2725/2000, 11 décembre 2000, JOUE n°L 316, 15 déc.

8.. Selon le Contrôleur européen à la protection des données (CEPD) « le système EURODAC est un élément clé dans la procédure suivie par chaque demandeur d'asile de l'UE dont les empreintes digitales sont relevées ».

9.. Décision 2004/512/CE du Conseil, du 8 juin 2004, portant création du système d'information sur les visas (VIS) [Journal officiel L 213 du 15.06.2004].

10.. Loi « Debré » n°97-396 du 24 avril 1997.

11.. Mariani T., *Rapport d'information sur la mise en application de la loi n°2003-1119 du 26 novembre 2003 relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité*, 1er mars 2006.

12.. Délibération n°96-417, 15 mai 1996, art. 1er, JO, 18 mai.

13.. Le fonctionnement en dehors de tout texte de ces fichiers a été régularisé par la loi sur la sécurité intérieure n°2003-239, 18 mars 2003, JO, 19 mars, qui a permis de plus leur accès aux autorités dans le cadre de simples enquêtes administratives. Le STIC avait déjà été régularisé en 2001, le JUDEX ne l'a été qu'en 2006 : Décret n°2006-1411 du 20 novembre 2006 portant création du système judiciaire de documentation et d'exploitation dénommé « JUDEX » JO, 22 nov.

14.. Régularisé par un décret n°87-249, 8 avril 1987, mod. par D. n°2005-585, 27 mai 2005 : JO, 29 mai.

15.. Géré à Ecully (Rhône), près de Lyon, à la sous-direction de la police technique et scientifique, le FNAEG (Fichier national automatisé d'empreintes génétiques) a été créé par la loi n°98-468 du 17 juin 1998 relative à la répression des infractions sexuelles ainsi qu'à la protection des mineurs.

16.. Voir par exemple l'article « La tentation du fichage de masse », *Le Monde*, 26 septembre 2006.

17.. « Tout homme étant présumé innocent jusqu'à ce qu'il ait été déclaré coupable, s'il est jugé indispensable de l'arrêter, toute rigueur qui ne serait pas nécessaire pour s'assurer de sa personne doit être sévèrement réprimée par la loi ».

18.. Rivero J., *Les Libertés publiques*, t. 2, « Le régime des principales libertés », p. 21, Paris, PUF, coll. « Thémis », 2003.

19.. Hobbes T., Léviathan. *Traité de la matière, de la forme et du pouvoir ecclésiastique et civil*, (1651), université du Québec, Chicoutimi, http://classiques.uqac.ca/classiques/hobbes_thomas/leviathan/leviathan.html

20.. Voir par exemple cette position dans Foessel M., « La sécurité : paradigme pour un monde désenchanté », *Esprit*, aout-septembre 2006, p. 194.

21.. Nous n'entrerons pas dans le débat classique en période de crise : est-ce en développant une politique de sécurité qui bafoue ses principes ou en ne se protégeant pas

au nom de ses principes que la démocratie court le risque de détruire ses propres fondements ? « Les démocraties, les Etats de droit peuvent se détruire faute de se défendre, ou en s'exposant trop, en ne se protégeant pas assez ; ils peuvent aussi se détruire en reniant leurs propres principes, en dérogeant aux droits fondamentaux, en instaurant des états d'exception qui se pérenniseront pour donner lieu à des Etats policiers, à des dictatures », Monod J.-C., « Vers un droit international d'exception ? », *Esprit*, août-septembre 2006, p. 186. La question très actuelle du recours à la torture par un pays démocratique au nom de sa sécurité est au cœur de cette interrogation.

22.. Arrêt Klass c/RFA du 6 septembre 1978, Leander c/Suède, 26 mars 1987.

23.. Rotaru c/Roumanie, 4 mai 2000.

24.. Segersted-Wiberg et autres c. Suède, 6 juin 2006 (requête n°62332/00) : « La conservation de données personnelles ayant trait à des opinions, tendances ou activités politiques qui a été jugée injustifiée au regard de l'article 8 § 2 constitue ipso facto une ingérence injustifiée dans l'exercice des droits protégés par les articles 10 et 11 ».

25.. Voir par exemple : Décision n°2003-467 DC 13 mars 2003, Loi pour la sécurité intérieure (JO du 19 mars 2003).

26.« L'ensemble des garanties prévues par les articles 21 à 23 de la loi pour la sécurité intérieure, ainsi que celles de la loi du 6 janvier 1978, qui, comme il ressort des débats parlementaires, s'appliquera aux traitements automatisés de données nominatives mis en oeuvre par les services de la police nationale et de la gendarmerie nationale dans le cadre de leurs missions, sont de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée », Décision n°2003-467 DC 13 mars 2003, cons. 21 à 27, J0 du 19 mars 2003, p. 4789.

27.. « Les principaux critères de limitation des droits de l'Homme dans la pratique de la justice constitutionnelle », 8e séminaire des Cours constitutionnelles tenu à Erevan du 2 au 5 octobre 2003.

28.. Charte de l'environnement de 2004.

29.. « Toute personne a droit à la protection de sa vie privée et familiale, de son domicile et de sa correspondance ».

30.. Kruslin 1990 ; Vetter c. France n°59842/00, 31 mai 2005.

31.. Il faut relativiser la différence de conception entre les pays européens : ainsi, depuis l'incorporation de la Convention européenne au Royaume-Uni avec le Human Rights Act de 1998, la conception de la vie privée élaborée par la Cour européenne des droits de l'Homme s'y impose progressivement.

32.. Technologies fondées sur la biométrie, Rapport non classifié, OCDE 10 juin 2005, Direction de la science, de la technologie et de l'industrie, Comité de la politique de l'information, de l'informatique et des communications, Groupe de travail sur la sécurité de l'information et la vie privée.

33.. Voir dans ce numéro notre article « L'Union européenne et les technologies de sécurité ».

34.. Art. 2 loi 6 janvier 1978 modifiée – Art 2 Directive 24 octobre 1995 : « toute information concernant une personne physique identifiée ou identifiable ». Est réputée identifiable, selon la directive, « une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification, ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ». Un arrêt « Durant » de cour d'appel britannique suivi par l'Autorité de contrôle a toutefois restreint cette définition,

aboutissant à faire échapper à la protection un nombre considérable de données : « ne peuvent être considérées comme des “données relatives à une personne”, au sens de la loi et de la directive, que des données de nature “biographique” ou véritablement “centrées” sur la personne concernée », in CNIL, rapport d'activités 2005, p. 85.

35.. « (16) considérant que les traitements des données constituées par des sons et des images, tels que ceux de vidéo-surveillance, ne relèvent pas du champ d'application de la présente directive s'ils sont mis en œuvre à des fins de sécurité publique, de défense, de sûreté de l'Etat ou pour l'exercice des activités de l'Etat relatives à des domaines du droit pénal ou pour l'exercice d'autres activités qui ne relèvent pas du champ d'application du droit communautaire ».

36.. Délibération n°2005-208 du 10 octobre 2005 portant avis sur le projet de loi relatif à la lutte contre le terrorisme ; Loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, JO, 24 janvier.

37.. Ex : Décret du 25 avril 2006 modifiant le décret n°2004-1266 du 25 novembre 2004 portant la création à titre expérimental d'un traitement automatisé des données à caractère personnel relatives aux ressortissants étrangers sollicitant la délivrance d'un visa BIODEV (JO 26 avr.), pris contre l'avis négatif de la CNIL en date du 20 décembre 2005 ; le « Fichier des hébergeants » a été créé par le D. n°2005-937 du 2 août 2005 pris pour l'application de l'article L. 211-7 du code de l'entrée et du séjour des étrangers et du droit d'asile et portant sur le traitement automatisé de données à caractère personnel relatif aux demandes de validation des attestations d'accueil (JO 6 août) malgré la délibération de la CNIL n°2005-052 du 30 mars 2005 (demande d'avis n° 1 046 585, JO, 6 août).

38.. ADP : Aéroports de Paris, organisme chargé de la gestion des aéroports français.

39.. Voir dans ce numéro notre l'article « L'Union européenne et les technologies de sécurité ».

40.. Article 13 : « Exceptions et limitations : 1. Les Etats membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6 paragraphe 1, à l'article 10, à l'article 11 paragraphe 1 et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder : a) la sûreté de l'Etat ; b) la défense ; c) la sécurité publique [...] ».

41.. « (13) considérant que les activités visées aux titres V et VI du traité sur l'Union européenne concernant la sécurité publique, la défense, la sûreté de l'État ou les activités de l'État dans le domaine pénal ne relèvent pas du champ d'application du droit communautaire ».

42.. Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée à Strasbourg, 28.1.1981.

43.. Voir par exemple l'intervention d'Alex Turk, ancien président de l'autorité de contrôle Europol (et Schengen), « Malheureusement, cette autorité souffre de trois faiblesses importantes. [...] En deuxième lieu, l'Autorité est financée directement par Europol. Enfin, les administrations nationales et Europol ont tendance à développer des relations en dehors du cadre de la Convention », Rapport fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du règlement et de l'administration générale (1) sur la proposition de résolution présentée par M. Hubert HAENEL au nom de la délégation pour l'Union européenne, en application de l'article 73 bis du Règlement, sur le projet de protocole modifiant la Convention Europol proposé par le Danemark (E 2064), 12 nov. 2003. Voir aussi note 2.

44.. Proposition de Décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale {SEC(2005) 1241}, 4.10.2005.
45.. Philippe Wolf est responsable du Centre de formation de la Direction centrale de la sécurité des systèmes d'information, DCSSI. Wolf P., « De l'authentification biométrique », *Infosécu*, n°46, octobre 2003.
46.. « Il est plus facile de comprendre le fonctionnement de la biométrie que d'appréhender les subtilités des technologies mathématiques cryptographiques ».
47.. Organisation de l'aviation civile internationale.
48.. Voir dans ce numéro notre article « L'Union européenne et les technologies de sécurité ».
49.. *Ibid*., à propos du Traité de Prüm.
50.. Wolf P., *op. cit*.
51.. Il est impossible de ne pas tenir compte du marché très porteur des technologies de sécurité, et de l'intérêt des entreprises en matière de choix des Etats, question traitée dans Les Technologies de sécurité, rapport Gendarmerie, septembre 2005.
52.. http://www.fidis.net/fileadmin/fidis/press/budapest_declaration_on_MRTD.fr.pdf
53.. Règlement (CE) n°460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information, JOUE du 13.3.2004, L 77/1. L'implication des entreprises privées en matière de sécurité des systèmes et de l'information pose des questions délicates dans le cadre des grands fichiers de sécurité européens et nationaux.
54.. *Biometrics at the Frontiers, Assessing the Impact on Society*, Rapport EUR21685, 2005, IPTS, Commission européenne.
55.. Voir note 29.
56.. Voir le Rapport CNIL 2005.
57.. Communication de la Commission au Conseil et au Parlement européen sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases, 24.11.2005 COM(2005) 597 final.
58.. Proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité du 12.10.2005 (COM(2005)490 final ; Avis du Contrôleur européen de la protection des données, JOUE, C 116/8, 17.5.2006.
59.. *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*, 2003, The Institute for Prospective Technological Studies (IPTS).
60.. Voir en ce sens l'article de Bioy X., « L'identité de la personne devant le Conseil constitutionnel » in *Revue française de droit constitutionnel*, n°65, janvier 2006, p. 73.

RÉSUMÉS

Cet article traite des questions juridiques posées par les bases de données personnelles dans le cadre du recours aux technologies de sécurité, notamment en Europe. La relation entre sécurité et démocratie étant centrale, l'Union européenne a fait le choix de placer cette question sous

l'angle du respect des droits fondamentaux. Mais, si la protection de la vie privée et son développement sous forme d'une protection spécifique des données personnelles semble précise dans les textes, dans les faits, elle apparaît comme très formelle et peu efficace, surtout dans le cadre des fichiers de sécurité. A cela s'ajoute une série de dysfonctionnements techniques non résolus et des problèmes soulevés par la transformation des données biométriques en véritables données publiques, stockées dans un nombre considérable de systèmes informatiques. Ces risques sont renforcés par l'objectif d'interconnexion de l'ensemble des fichiers de sécurité au niveau européen.

This article examines the legal questions generated by personal databases in the context of the resort to security technologies, notably in Europe. Considering the security/democracy nexus as essential, the European Union has chosen to examine this question under the angle of the respect of fundamental rights. Although the protection of private life, and its development through a specific protection of personal data, seems clearly defined in the texts, in practice it appears very formal and little efficient, especially concerning security files. Moreover several unresolved technical malfunctionings and problems generated by the transformation of biometrical data into public data stored in a considerable number of electronic systems. These risks are intensified by the objective of interconnection of all the security files at the European level.

INDEX

Mots-clés : bases de données, libertés publiques, protection

AUTEUR

SYLVIA PREUSS-LAUSSINOTTE

Sylvia Preuss-Laussinotte est maître de conférences en droit public à Paris-X Nanterre, directrice du Master 2 « Droit des nouvelles technologies et Société de l'information », et titulaire d'un DEA de sociologie de l'EHESS.